IJEMD-CSAI, 2 (2) (2023), 19 – 33
https://doi.org/10.54938/ijemdcsai.2023.02.2.662

IJEMD

International Journal of Emerging Multidiciplinaries: Computer Science & Artificial Intelligence

Research Paper
Journal Homepage: www.ijemd.com
ISSN (print): 0000-0000



An Edge-to-Access Secure Framework for Privacy-Aware Urban Surveillance

Wong Leong Hin [1], Kyle Adam Frank[2], Kosei Yamashita[3], Kros Anntonio Pereira[4], Julian Wong Yi Kai[5], Joel Wee Nambiar[6], Prashandt Henry[7], Siva Raja Sindiramutty[8]

[1]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0366319@sd.taylors.edu.my
[2]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0365830@sd.taylors.edu.my
[3]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0369113@sd.taylors.edu.my
[4]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0365595@sd.taylors.edu.my
[5]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0368830@sd.taylors.edu.my
[6]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0369032@sd.taylors.edu.my
[7]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia 0367977@sd.taylors.edu.my
[8]School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia siva.sindiramutty@taylors.edu.my

ARTICLE INFO

Submitted:
15-09-2023
Revised:
30-10-2023
Accepted:
15-11-2023
Keywords:
Privacy-by-Design Surveillance, Edge Anonymization, Smart City Security, Blockchain Audit Logging, Role-Based Access Control (RBAC).
***Corresponding Author**:* Wong Leong Hin
0366319@sd.taylors.edu.my

ABSTRACT

As smart cities increasingly rely on IoT-enabled surveillance for public safety, the industry-standard practice of streaming raw footage to centralized cloud servers has introduced critical vulnerabilities regarding data privacy and accountability. Current "collect-first, protect-later" architectures create massive targets for cyberattacks and unauthorized administrative access. This report will propose an exceptional, three-layer security framework which consists of the Edge Layer, the Cloud Layer, and the Access Layer. Our particular design is to introduce a "Privacy-by-Design" methodology. At the Edge Layer, we implement an atomic, real-time anonymization process using lightweight deep learning models like YOLO (You Only Look Once), BlazeFace, and Reversible Chaotic Masking. This ensures that Personally Identifiable Information (PII) is redacted in ephemeral memory before network transmission, effectively neutralizing Man-in-the-Middle attacks. The Cloud Layer secures data that is not being transmitted via AES-256-GCM and ensures model integrity through OpenSSF Model Signing. Crucially, the Access Layer addresses the risk of data breaches and unauthorized access by utilizing Role-Based Access Control (RBAC) with a blockchain-based immutable audit ledger. To address hardware constraints, like a device with outdated hardware, this system utilizes Particle Swarm Optimization (PSO) for intelligent task offloading. After extensive comparisons, we can confirm that this holistic approach offers superior privacy protection, bandwidth efficiency, and forensic non-repudiation compared to other existing centralized surveillance models.

1.Introduction

Smart cities across the globe have a detailed history of developing secure systems, integrating information and communication technologies (ICT) and Internet of Things (IoT) devices to optimize various services that greatly streamline & advance the maintenance strategies of these cities. These urban services include traffic management, healthcare coordination, general infrastructure monitoring and so on. These systems also rely on complex networks made up of sensors, surveillance devices and cloud-based analytics to support frequent and efficient maintenance.

However, as these environments advance technologically, cyberattacks are gaining a larger and broader chokehold on system vulnerabilities. This is especially critical in the domain of surveillance of smart cities, as the vast networks of cameras required for public safety inadvertently creates a wider attack surface for attackers. With that being said, ensuring the security of these smart systems is crucial to maintaining the privacy, anonymity, and sustainability of smart cities and its citizens (Sanjaya et al., 2025; Ismail et al., 2021). Despite ongoing advances, current approaches are often prone to real-time threats and scalability issues. This report will specifically address the glaring issue of anonymity in smart city cameras, analyzing the critical privacy risks introduced when raw, identifiable footage is continuously transmitted to centralized cloud storage.

Specific Security Problem

Within the domain of Secure Systems for Smart Cities, the specific security problem lies in how cities manage visual data that is captured by public surveillance systems. Nowadays, smart city infrastructures increasingly

© 2023 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). https://creativecommons.org/licenses/by/4.0/

depend on CCTV cameras, drones, and IoT-enabled sensors to enhance aspects like safety, flow of traffic, and overall operational efficiency. These devices continuously capture high volumes of real-time video footage that often contain Personally Identifiable Information (PII) like facial features, vehicle license plates, and recognizable behavioral patterns (Jacob et al., 2021; Jhanjhi, 2025). These systems are deemed essential for the public. However, it also introduces its own challenges too. Mainly risks of privacy leaks and surveillance abuse of the PIIs captured. Hence, the rights of individuals and the integrity of the systems are compromised.

The issue comes from the storage and management of raw video data in centralized cloud infrastructures. Since the footage is available to the public, it is seen that the footage can also be accessed by users with malicious intent. "Centralized footage storage systems in smart cities can lead to increased privacy risks. This is because once raw visual data is uploaded, it can be accessed, retained, and repurposed by a wide array of users (de Oliveira, de Melo, & Zaharia, 2022; Khalil et al., 2021). This can lead to privacy breaches and surveillance abuse, especially when proper encryption, access control, and anonymization mechanisms are not in place. At the same time, citizens are rarely informed about when or how their movements are being tracked, and the lack of transparent governance around data collection further deepens public mistrust (Zoonen, 2016; Loveleen et al., 2022).

Diving deeper, these systems are architected to be efficient and powerful for analytics, putting user consent and data minimization way down the priority list. What often happens is that cameras and sensors just send raw, unfiltered footage straight to the cloud, where it's hoarded and then analyzed for purposes far beyond its original intent. Situations like this can lead to behavioral profiling, or even selling the data for profit (Chen & Lee, 2023; Riskhan et al., 2025).

In short, integrating all this surveillance into cloud-based smart cities has created a real issue that actually contradicts the original intention of surveillance in the first place which is to ensure safety of citizens. The core issue is that privacy simply wasn't built into the foundation of most smart city video systems (Smith, 2021; Ying et al., 2024). It is apparent that cities want these systems for efficiency and protection, but citizens are now facing the ever-present risk of constant monitoring and data misuse. If we do not mitigate this issue, more citizen-centric smart cities will ultimately be ruined by unchecked surveillance and systemic privacy violations.

Inadequacy Of Current Solutions

Despite significant technological advancements in the systems securing smart cities, a critical area of protection, which is personal privacy, remains static. The prevailing data security framework adheres to a "collect now, protect later" model, a reactive paradigm that fails to address the root cause of privacy risk. Current solutions are designed to protect raw, sensitive data only after it has been collected and centralized, rather than proactively preventing the exposure of that sensitive data in the first place. The core inadequacy of this approach is the failure to anonymize video "at the edge."

This practice of transmitting raw, unfiltered video to cloud-based storage creates a highly concentrated, high-value target for hackers. The risk profile of this centralized model is clearly exemplified by the deployment of portable body-worn cameras (BWCs) in law enforcement. In a typical workflow, video and audio are captured in the field and the raw, unfiltered data is uploaded directly to the cloud. While the data is accessible to authorized personnel through a secure web portal, their model prioritizes convenience over security. It offers the perceived benefit of easier IT management with no local servers or firewalls to protect, but this convenience comes at the cost of exceptionally high risk (i2c Technologies, 2022; Weiqi et al., 2024).

Smart cities, by design, thrive on the collection of vast volumes of data. Real-time traffic monitoring, biometric security, Personally Identifiable Information (PII), geolocation data, and behavioral patterns are all collected at an unprecedented scale. The "collect now, protect later" model compounds this risk, as even data that is eventually anonymized can often be re-identified. According to an analysis by (*Protecting Personal Data in Smart Cities: The Role of Privacy Tech | TrustArc*, 2024), the aggregation of data from various sources creates a significantly increased risk of individual identification, even if personally identifiable details are initially stripped away. This vulnerability to re-identification highlights the fundamental flaw in current solutions: by failing to anonymize data at the point of capture, they create a permanent and irreversible privacy risk before the first layer of security is ever applied.

With all the technological advancements that have been made to secure the systems for smart cities, there is one area in protection where it is still at a standstill. Most solutions are stuck in a "collect now, protect later" model, which fails to address the root cause of the privacy risk (Kuktelionis, 2024; Sindiramutty, Tan, & Wei, 2024).

The current solutions are reactive, **not proactive**. They are designed to only protect raw, sensitive data after it has already been collected and centralized, rather than preventing the exposure of that sensitive data in the first place. The core inadequacy is that current solutions do not anonymize video at the source to the edge (Leong, 2023).

Recent Real-World Incidents

Recent real-world incidents illustrate significant vulnerabilities in public digital infrastructures. In a notable cyber-attack, storage devices containing data from Washington, D.C., police surveillance cameras were compromised with ransomware just eight days before the 2017 presidential inauguration (Williams, 2017). According to a criminal complaint, two individuals hacked 123 of the Metropolitan Police Department's 187 outdoor surveillance cameras by infecting the connected computers with ransomware in an effort to extort money (Khandelwal, 2017). The attack occurred just days before the inauguration of President Donald Trump and left the cameras unable to

record for nearly four days. Instead of paying the ransom, the D.C. police took the storage devices offline, removed the infection, and rebooted the systems to restore full operation.

On another separate occasion, the MySejahtera data breach in Malaysia in which three million users' personal data was exposed, illustrates how poor data governance, weak security configurations, and the absence of strict oversight can lead to massive exposure of sensitive information (CodeBlue, 2023; Sindiramutty, Prabagaran, Akbar, et al., 2024a). While MySejahtera did not directly involve video data, it represents a broader failure in ensuring citizen data confidentiality in government-managed digital systems, a pattern that can easily extend to smart city surveillance infrastructures. The incident highlights that technical safeguards alone are insufficient without strong policies for accountability, transparency, and ethical data usage.

2. Literature review & Gap analysis

Review Of Sources

This section provides a critical review of the existing literature on security and privacy within smart city video surveillance systems from ten different sources. The review is structured around three core themes: the evolution of video anonymization techniques, the mechanisms for controlling access to sensitive data, and the methods for ensuring system auditability.

(Li et al., 2021). proposed a security framework for surveillance video protection which implements a robust and protected encryption key management mechanism through Chinese Remainder Theorem. The proposed solution primarily addresses Man-in-the-Middle attack with the help of Diffie-Hellman key exchange protocol as its authentication model. This approach ensures transparency in the authorization process and simultaneously prohibits malicious duplication and modification of the original video data.

(Gao et al., 2025; Sindiramutty et al., 2024). reviewed the chaos-based encryption for its benefits to video data encryption and decryption. The chaos-based encryption stems originally from the discovery of the butterfly effect whereby a small change in one variable radically produces a different output. This cryptosystem injects non-linear, chaotic mappings into three stages of video processing: frame-sequence computation, pixel-level diffusion, and keystream generation. This application yields richer data diffusion than traditional encryption schemes while leaving less area for exploiting because of the safeguarded three layers throughout the video processing.

(Zhu et al., 2022). presented a hybrid sensing system of crowdsensing and IoT sensing, where individuals are incentivized to provide their data through a credit system while preserving their data privacy. This system minimizes data leakage from IoT devices as well as users' edge device vulnerabilities in complementary manner. The former challenge is addressed by physically obscuring them so that private user data is inaccessible, and the latter concern is handled by each edge device being incorporated with a blurry hardware filter. Throughout this report, hardware security measures are frequently practiced due to their predictable performance over software-based approach.

(Kanwal et al., 2020). Proffered a methodology in preserving a chain-of-evidence, which is proof of the authenticity in surveillance videos, which is efficient in terms of computation by means of hashing and steganography. Salted hash as a digital signature is appended over every single frame of a video, and to be compliant with GDPR, the entire video frames are encrypted on the network edges closer to the recording device itself, without reliance on cloud storage or transmission over a wide area network. The uniqueness of the offered framework is that it is not only GDPR compliant but also deployable in resource-constrained nodes such as Raspberry-Pi processors as used in the study's experiments.

(Akhuseyinoglu & Joshi, n.d.). reviewed existing solutions and challenges of access control in the modern IoT devices. There are currently many existing Access Control mechanisms for IoT that are centralized. Mainly to compensate for weaker devices. This approach has drawbacks that require a frequent exchange of messages and consumes a lot of resources which makes it scarce. The solutions are to use a Trust-aware Access Control system for the IoT (TACIoT), which is built on Distributed Capability-Based Access Control (DCapBAC). This model uses tokens as capabilities, allowing a device to access resources multiple times without needing to re-evaluate the policies which save resources. Towards the end, the author believes that by leveraging blockchain technology and its promise for decentralized trust, distributed AC approaches can be a promising direction for AC in smart cities.

(Huh et al., 2025). proposed a similar idea which introduces an edge-cloud surveillance system that tackles the bandwidth strain and severe privacy risks of traditional full-footage transmission. The innovation lies in processing and anonymizing video right at the edge, where it uses 3D human models to replace identifiable features with abstract representations. This approach achieves real-time performance and good data compression. In comparison, it is over 5,000 times smaller than the raw video. All while successfully preserving more than 85% of the original scene context. The authors conclude that this intelligent edge-based anonymization is a highly effective model for developing privacy-aware and network-efficient smart city surveillance systems that limit the exposure of sensitive raw footage.

(Fitwi et al., 2021). proposed a Privacy-preserving Surveillance as an Edge Service (PriSE) which combines a video protection schema with a lightweight foreground object scanner. End-to-end protection is implemented through the Reversible Chaotic Masking. The proposed model places a strong emphasis on on-site edge pre-processing of captured video data in frame-by-frame manner, discarding meaningful foreground objects. At the

same time, objects of possible privacy concerns such as faces and windows are masked using the algorithm. Overall, this prototype aims to achieve efficient computation with privacy in mind, with its conclusion stating that it can maintain 5.12 fps on Raspberry Pi 4 combined with a simple motion detection scheme, indicating its feasibility in real deployment.

(Badidi et al., 2023). demonstrated the existing privacy frameworks in edge AI-assisted video analytics. This investigation primarily examines the power of machine learning based processing at edge level in its speed in detecting security breaches or quality issues. The research suggests that edge video analysis has superior security promises when isolated, as the data will be processed completely in the favor of the rules set on the local model, abandoning personal traits before submission over a wide area network.

A comparable research by (Giorgi et al., 2022) has explored a security framework in a privacy-preserving video surveillance system with consistent anonymization of video frame by frame. The demonstration ensures data confidentiality through communication with remote data analysis servers. This implementation model further aims at the balance between privacy and accuracy of the recorded medium, which is a common trade-off in video sanitization.

(Odeh & Taleb, 2025). proposed Blockchain-Enhanced Trust and Access Control for IoT Security (BETAC-IoT) model, which has been introduced to eliminate security concerns brought about from centralized data management such as single point of failure, network congestion, transparency and auditability. This model stands as a hybrid of several security frameworks including federated learning, blockchain, and Merkle Tree for enhanced transparency and predictable real-time performance, which is essential for our chosen scope. This solution specifically puts a strong emphasis on the nature of blockchain and Merkle Tree to compensate for the computational overhead, resulting in a highly scalable system of time complexity of Olog(n).

Gap and Limitations

After reviewing the sources, some proposed solutions guarantee auditability and data privacy, while overcoming performance and energy consumption issues through lightweight cryptographic algorithms and Proof of Authority. However, a few challenges have yet to be addressed such as unknown space complexity due to the growth in ledger-size, and compliance with regulations like General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA).

Other than that, as seen in the reviewed sources, the proposed solution often sacrifices computational overhead for the sake of privacy. This leads to greater anonymity and data protection one at a time, however it is not ideal for scalability. That could leave a door for security breaches, as it is not entirely guaranteed the completion of video anonymization at time.

Lastly, other underlying issues found in the review ignore inconsistency in computation of each edge device, especially each sometimes being heterogeneous. While at the theoretical level, these approaches offer stronger security and data confidentiality, implementation may face hardship from an economical perspective, especially machine-learning or AI-based anonymization. Furthermore, these technologies are still at the early stage of development, which suggests possible non-deterministic realization.

To conclude, there is a research gap in developing a hardware-agnostic, efficient security model for resource-constrained edge devices. To address it, in our research, we would propose a low-latency, hierarchical framework which incorporates three layers: edge layer, cloud layer, and access layer. At the edge layer, a lightweight, deterministic vision model is implemented for blurring and censoring privacy data. At the cloud layer, data anonymization and perturbation are done for reduction in entity uniqueness. Finally, at the access layer, Blockchain based audit logging system is introduced for transparency.

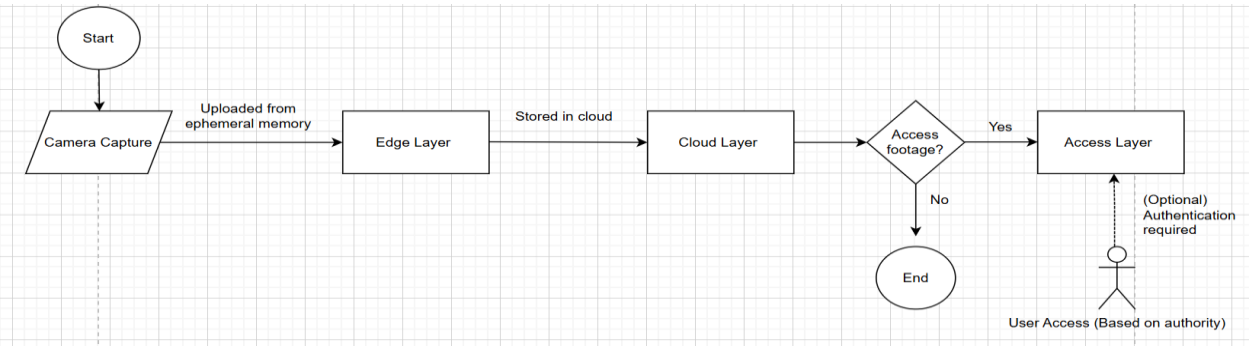
3.Proposed Secure System

Architecture Overview

In this section, we would propose our security framework powered by blockchain auditing and homogeneous machine learning models. There are mainly three layers; edge, cloud, and access, each being a standalone, composable module which prevents a single point of failure. These layers will be covered one by one from its architectural overview to implementation details. Finally, by incorporating existing research, we aim to demonstrate the primacy of our solution.

Below is a general overview of how raw footage that is captured gets processed through the layers within this proposed architecture.

Figure 1: Data Flow Diagram of the 3 Layer Architecture



The process starts when the camera in the smart-city camera records a clip, it is captured in standardized resolution at 1080p (1920x1080). We chose this configuration as an optimal midpoint based on the compromise between needing enough pixels for AI detection accuracy and computational efficiency for real-time optimization. This raw data is then temporarily handled through ephemeral memory which means the footage exists temporarily and it is automatically discarded after processing. This decreases the risk of unprotected data being leaked.

Once the footage is captured and uploaded from the ephemeral memory, it is transmitted through the edge layer. This is where processes such as facial blurring, object detection using YOLO version systems, and Face detection using BlazeFace by Google. The purpose of the layer is to ensure that the footage is securely anonymized before it gets uploaded to the cloud layer.

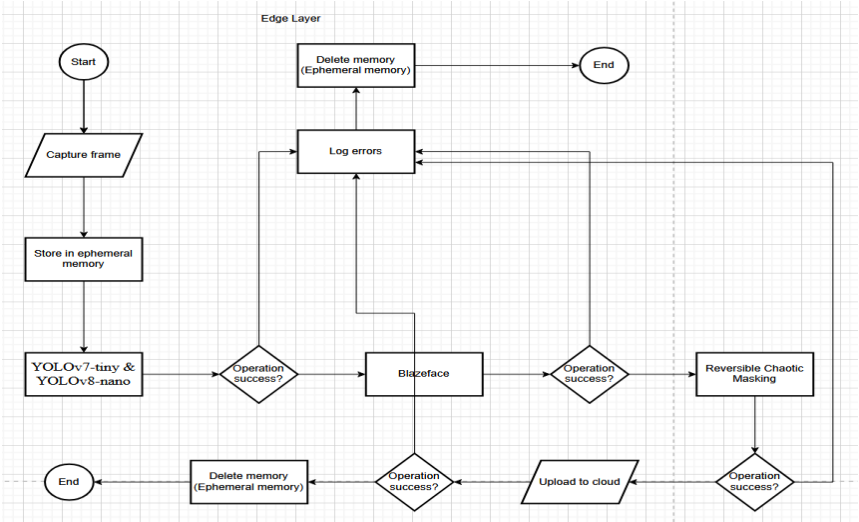
After that, the processed video is uploaded and stored in the cloud layer. By this point, footage is properly stored in a secure environment. Uploaded footage is protected using AES-256-GCM encryption, where it gives strong encryption and integrity verification to prevent unauthorized access or modification. TLS 1.3 encryption is also used to make sure footage cannot be intercepted or altered while being transmitted. Cryptographic keys such as Hardware-Security Module (HSM) and Short-lived key exchange mechanism are used to create a more secure environment. This ends both the anonymization and storing processes of the footage captured from the smart city.

Once this process has ended, authorized users will have the option to access the footage in the access layer. The access layer functions as a gateway so that access to the stored video data is secure and heavily role restricted. This layer consists of Blockchain-Based Audit and Role-Based Access Control (RBAC). These components will monitor access requests to the access layer as well as restrict unauthorized access. Whether from system administrators, or government enforcement each time the layer is accessed, it will be logged and be verifiable. Temporary access to unblurred content may be granted to authorized people with a strict Time-to-Live window to prevent misuse. These controls are crucial in making sure that the footage stays anonymous and that access can be traceable and justified.

The Edge Layer

The primary emphasis of edge layer is rather the atomicity of operation chaining than complete security, as edge devices typically lack powerful processing units to fully achieve the security computation. This layer acts as the most crucial line of defense for privacy. The core principles involved at this layer are atomic and ephemeral processing, guaranteeing the all-or-nothing frame-by-frame anonymization. The raw, identifiable video frames exist only in the ephemeral memory so that without the full completion of operation they are inaccessible at all, empowering the data confidentiality. Figure 2 presents the algorithmic flow at this layer, occurring at each frame processing.

Figure 2: Algorithmic Flowchart of the Edge Layer



The technologies selection is based on the optimal balance between the weight, security, and space complexity. There are three core processing schemes involved: YOLOv7-tiny, YOLOv8-nano, BlazeFace, and Reversible Chaotic Masking. Each of them is encapsulated under the veil of atomicity – as soon as any of the operation fails, the entire flow shifts to error logging followed by discard of the ephemeral memory. Otherwise, the anonymized frame will be uploaded to the cloud securely, then the deletion of the ephemeral memory takes place. The atomicity in each operation addresses the inherent inability and limited computational capacity of the implemented edge devices at the same time preventing error propagation.

The first combination of YOLOv7-tiny and YOLOv8-nano achieves object detection. These models offer significant advantages in accuracy compared to traditional models such as Haar Cascades, while being specifically designed for high resolution video on affordable edge devices including Raspberry Pi 4. Their compact architectures of less than 12 MB parameters minimize memory overhead, enabling efficient multi-object recognition under severe resource constraints.

The BlazeFace by Google then performs face detection which is ultimately optimized for mobile and edge platforms. By default, its size is around 1.5 MB which saves its own footprint and claims excellent and seamless integration in a multi-processing pipeline that is crucial without the additional GPU requirements.

Finally, the anonymization is achieved with the Reversible Chaotic Masking Algorithm. This, as talked about in the literature review, uses deterministic chaotic maps which generate pseudo-random sequences without requiring heavy integer arithmetic. This provides encryption-like protection with drastically lower computational cost compared to AES, DES, or RSA. While the security level achievable is not high, this trade-off is acceptable for its linear time complexity and low memory usage.

The entire process flow is yet heavy workload for heterogeneous edge devices, and to maximize the efficiency, we introduce task offloading through Particle Swarm Optimization (PSO). Edge devices then can make an intelligent, real-time decision to either process a frame locally or offload the detection task to a more powerful, nearby edge gateway or node. PSO helps optimize this decision based on network latency, node processing load, and power consumption, ensuring the entire system maintains real-time performance.

The Cloud Layer

At the cloud layer of our proposed system, we would assume there is no resource constraint thus providing infinite computational power. Data encryption, key management, and enhancement on data anonymization and perturbation are performed in this abstraction stack.

When an edge device submits an anonymized frame to the cloud, the transmission goes through the TLS 1.3 tunnel. Then as soon as the frame is stored, it gets encrypted using the AES-256-GCM Encryption scheme. This is the high-strength, industry-standard authenticated symmetric encryption used to protect the data at rest within the cloud storage and during complex computation. The GCM mode stands for a hybrid encryption scheme which consists of AES-CBC for confidentiality, and HMAC-SHA256 for integrity, doubling the complexity and increasing risk of implementation bugs. Furthermore, AES-GCM is supported in various hardware and strictly optimized for each platform so that it can reach the throughput of 10Gbps.

As this layer is encryption heavy, key management is another crucial aspect. We deploy our own Hardware Security Modules (HSMs) to securely generate, store, and manage the cryptographic keys required for AES-256-GCM and TLS operations. This physically protected environment prevents unauthorized access and manipulation of the master keys. In addition to key randomization, the keys can be automatically rotated by HSMs, making it even harder for a hacker to bypass them. Compared to Trusted Platform Modules (TPMs), HSMs are capable of more than encryption such as notifying the IT department whenever there is an attack from outsiders accessing the HSM.

In conjunction with HSMs, the system implements a short-lived key exchange between the edge layer and the cloud layer. This minimizes the exposure window if a session key is compromised, enhancing forward secrecy and overall system resilience. This mechanism is based on the Double Ratchet Algorithm which is a key management protocol used in two parties to exchange encrypted messages, in this case the anonymized frames, based on a shared key made with Diffie-Hellman calculations.

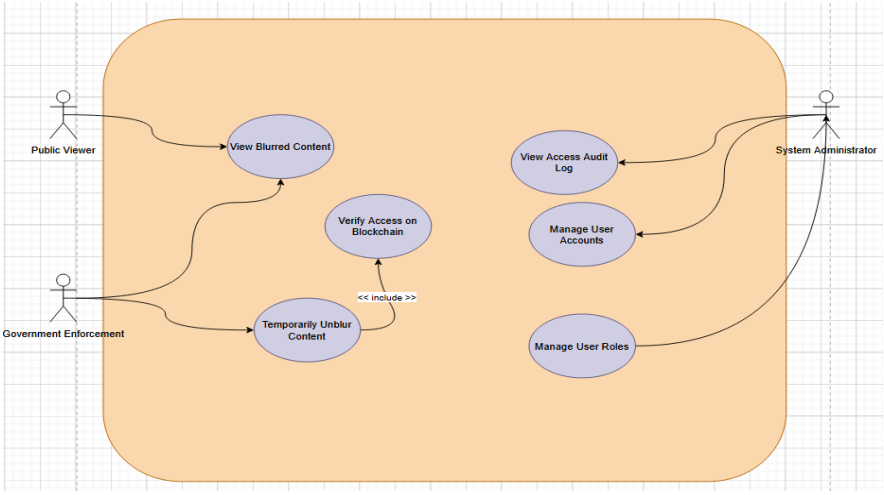
Finally, to ensure the anonymization models' homogeneity across the edge devices from the cloud layer, we incorporate OpenSSF Model Signing, which is a protocol crucial for establishing and verifying the integrity and authenticity of machine learning models running on the cloud and edge. Since complex computation (e.g., advanced video analytics, facial recognition) is assumed to happen here, model signing prevents the execution of malicious or tampered models (a form of supply chain attack).

The Access Layer

As for the access layer of our system, it will serve as a secure interface between the system's data and the human operators. The access layer of our proposed system is primarily responsible for the authentication and authorization of users. Mainly the Public Viewer, Government Enforcement, and System Administrator.

Our proposed access layer introduces a robust Blockchain-Based Audit Mechanism integrated with strict Role-Based Access Control (RBAC). This ensures that even though the public viewer is able to view a part of the system, it retains forensic capabilities for law enforcement and the system administrators without sacrificing the rights of the public. The roles will be shown below:

Figure 3: Use Case Diagram of the Access Layer with Role-Based Access Control (RBAC)



As shown in the use case diagram above, both the Government Enforcement and the Public Viewer share the "View Blurred Content" use case. This further enhances our standard where all video feeds remain anonymous unless a very specific operation arises. Additionally, the Government Enforcement will not be able to execute "Temporarily Unblur Content" unless the "Verify Access on Blockchain" use case completes successfully. This ensures data privacy for the public and ensures that only verified government enforcements and only government enforcements are able to view unblurred content.

All in all, Public Viewers will only be able to view fully obfuscated videos. Government Enforcement will only have conditional access to viewing unblurred content only if they have proper credentials like case number assignment and so on. Even if they are able to view unblurred content, there is a specific Time-to-Live (TTL) window. Finally, the System Administrator will be able to manage what users are able to access in the system, check server health, and configure network routes.

4.Experimental Setup / Comparative Analysis

The foundational challenge in modern Smart City surveillance is the lack of integration between security solutions. Existing state-of-the-art models typically focus either exclusively on protecting data at the source (privacy) or securing the backend rules (integrity), creating critical systemic vulnerabilities. Our proposed 3-Layer Secure System is designed as a holistic framework to bridge these architectural and ethical gaps.

To validate our architectural necessity, we benchmark our comprehensive framework against two leading and contrasting security models that represent the current best standards in isolated domains:

System 1 (Edge-Focus): Focuses on Proactive Privacy and Traffic Efficiency via 3D models and masks. Its critical deficiency is Accountability, as it lacks a tamper-proof audit log and granular access control (RBAC).

System 2 (Backend-Focus): Focuses on Integrity and Trust via AI and Smart Contract verification. Its critical deficiency is Proactive Privacy, as it fails to prevent raw PII capture and exposure at the edge node.

Comparative Analysis

Comparison 1: Against Edge-Focused Privacy (System 1)

Reference System: A Novel Intelligent Video Surveillance System Using Low-Traffic Scene-Preserving Video Anonymization (Huh et al., 2025).

This system represents a major advancement in data abstraction, utilizing an edge-cloud architecture where the edge node extracts compressed scene information via 3D human models and segmentation masks.

Strengths of System 1 (And Our System's Overlap)

System 1 demonstrates significant efficiency by achieving a significant bandwidth reduction compared to raw video transfer through the transmission of highly compressed parametric models.(Huh et al., 2025) Our proposed system leverages this same core concept, specifically transmitting YOLO and BlazeFace parameters, to ensure comparable network traffic efficiency suitable for bandwidth-constrained smart cities. In terms of performance, the system runs in real-time at greater than 30 FPS on typical hardware settings, validating the operational feasibility of our proposed Edge Layer for high-speed inference without inducing latency. Additionally, it ensures privacy protection by preventing identity reconstruction unless specific "blend shapes" stored securely on the cloud are accessed, thereby demonstrating a strong scene-preservation correlation of over 85% (Huh et al., 2025).

B. The Critical Gap (Our Advantage: Accountability) System 1 addresses the technical risk of video leakage but ignores the ethical and policy risk of authorized misuse. Specifically, the system relies on a conventional cloud server and administrator database (Huh et al., 2025), making it vulnerable to a "rogue administrator" attack where an individual with high-level privileges could access or delete access logs without facing an unavoidable, independent accountability mechanism. Furthermore, the architecture fails to detail advanced, real-world access

policies, lacking the necessary Role-Based Access Control (RBAC) implementation required by city authorities to differentiate access rights between various stakeholders, such as traffic engineers and police investigators.
Conclusion on System 1 Our solution builds upon System 1's technical success in efficiency and anonymization by integrating a Blockchain-Based Audit Mechanism in the Access Layer. This enhancement ensures that all data access and de-anonymization requests are transparently and immutably logged, filling the critical accountability gap overlooked by a purely edge-focused model.

Comparison 2: Against Backend-Focused Integrity (System 2)

Reference System: Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges (Gupta et al., 2020).
This research focuses on securing the core logic of decentralized systems by using Artificial Intelligence (AI) to mitigate software vulnerabilities inherent in Smart Contracts (SCs).

Strengths of System 2 (And Our System's Overlap)

System 2 directly addresses the vulnerabilities, such as re-entrancy and integer overflow, inherent in the software code of Smart Contracts, which is critical for our system that relies on blockchain for enforcement. Additionally, it proposes traditional security schemes like Trusted Execution Environments (TEE), Secure Multi-Party Computation (SMPC), and Zero-Knowledge Proof (ZKP) to enhance privacy(Gupta et al., 2020); similarly, our proposed Cloud Layer adopts these TEE principles, specifically by using Hardware Security Modules (HSMs), to enhance the security of data-at-rest
B. The Critical Gap (Our Advantage: Proactive Privacy) System 2 is a purely reactive, backend-centric solution. It focuses on protecting data and transactions after they have entered the blockchain ecosystem. (Gupta et al., 2020)
System 2 neglects edge privacy because its entire focus is on securing the processing of data and contractual rules; this approach fundamentally ignores the initial, pervasive privacy violation that occurs when a smart city camera captures and transmits raw PII to the network. So, without a dedicated Edge Layer for anonymization, raw PII must be exposed to the sensor's memory, network, or initial storage before the blockchain and AI security layers can be applied, creating a critical "vulnerability window" where raw footage could be intercepted before the Smart Contract begins its enforcement.
Conclusion on System 2 Our system achieves privacy-by-design superiority by addressing the privacy violation at time zero. Our Edge Layer guarantees that raw PII exists only in temporary memory during the atomic anonymization process. This ensures raw PII is never transmitted or stored in an identifiable format for the backend to handle, eliminating the initial privacy risk that reactive, backend-only security models like System 2 cannot solve.

Experimental Benchmarking Plan

A robust experimental plan is required to empirically validate these comparative claims. The methodology detailed below defines quantifiable metrics across Performance, Efficiency, Privacy, and Accountability to rigorously test the proposed architecture against existing solutions.

Performance and Efficiency Benchmarking (vs. System 1)

To evaluate performance and efficiency, the primary metrics will be Edge Processing Latency (ms) and Throughput (FPS). The experimental method involves measuring the time required to execute the complete "Atomic Operation" which includes frame capture, object detection, anonymization, and upload on a simulated edge node, such as a Raspberry Pi 4. The objective is to match or exceed the 25 FPS benchmark established by System 1. Achieving this target would prove that the added security complexity of integrating YOLO and BlazeFace models does not hinder the system's ability to perform real-time surveillance operations.

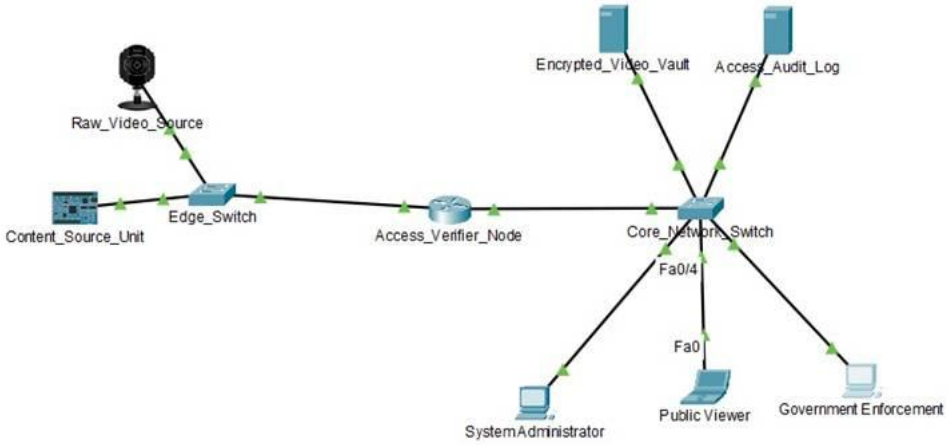
Traffic Efficiency Benchmarking (vs. Raw Stream)

Traffic efficiency will be assessed by calculating the Data Compression Ratio. This method involves determining the precise ratio between the file size of the raw video (encoded in H.264) and the size of the transmitted metadata, which consists of the parametric model data and the compressed segmentation mask. The experimental target is to achieve a compression ratio comparable to System 1's standard of 5,000:1. Meeting this target will validate that the proposed system significantly reduces bandwidth strain on Smart City networks compared to traditional video transmission.

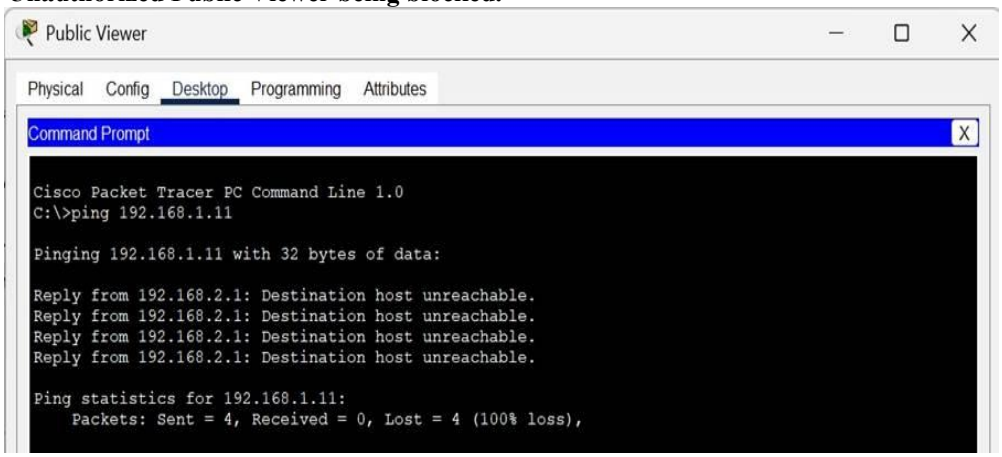
Integrity & Accountability Benchmarking (vs. System 1 & 2)

Benchmarking for integrity and accountability will focus on two distinct metrics: the Audit Log Immutability Score and Access Granularity. First, immutability will be tested using a binary score (0 or 1) by simulating a "Rogue Admin" attack where a privileged user attempts to delete an access log entry. The target is for the proposed blockchain-based system to achieve a score of 1 (Immutable and Distributed), whereas System 1's centralized database is expected to score 0, demonstrating superior accountability. Second, Access Granularity will be measured by quantifying the number of distinct, verifiable Role-Based Access Control (RBAC) policies that can be programmatically enforced across Public, Enforcement, and Admin roles. The goal is to demonstrate a higher number of specific, enforced policies compared to the generic access controls found in many research systems, thereby proving real-world deployability.

Proactive Privacy Benchmarking (vs. System 2)
Finally, proactive privacy will be benchmarked against System 2 using the PII Exposure Risk Score and Scene Preservation Correlation. The exposure risk will be scored qualitatively based on the "vulnerability window" specifically, the duration and location of raw PII existence. The target is to demonstrate that the proposed system achieves a Near-Zero Vulnerability status by confining raw PII to ephemeral RAM for less than 40ms, eliminating the high vulnerability inherent in System 2 where raw data exists during transmission to the contract. Additionally, scene preservation will be validated by using human assessors to rate a "Risk Score" for both original and anonymized video streams to calculate the statistical correlation coefficient. The target is to maintain a correlation of greater than 85% (Huh et al., 2025), proving that the anonymization process does not hinder the core function of identifying risks and dangerous situations.
Simulation Environment To validate the 3-layer security architecture, a simulation was constructed in Cisco Packet Tracer 8.2 (see **Figure 4**). The topology strictly isolates the "Edge Layer" (Content_Source_Unit) from the "Access Layer" (User Terminals). This segmentation ensures that raw surveillance data is separated from the public network, forcing traffic through a central checkpoint.
Figure 4: Network Topology showing the segmentation between Edge, Cloud, and Access layers.

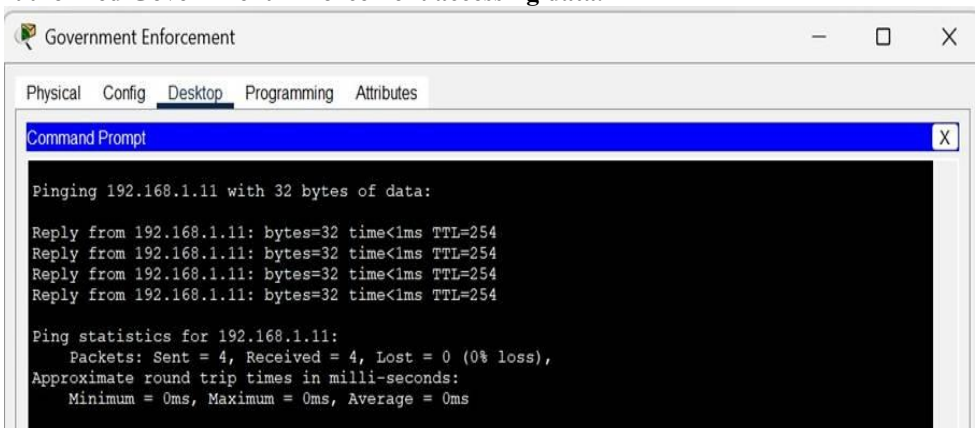


Security Configuration (ACL) The security logic is enforced by the central Access_Verifier_Node. An ACL named SECURE-CITY was configured to simulate "Smart Contract" verification. This firewall explicitly **denies** traffic from the Public Viewer while **permitting** traffic from Government Enforcement and the System Administrator for their specific roles.
Experimental Results Connectivity tests confirmed the effectiveness of the ACL. First, the Public Viewer was blocked from accessing the content source, receiving a "Destination Host Unreachable" message (**Figure 5**), proving user privacy is active.
Figure 5: Unauthorized Public Viewer being blocked.



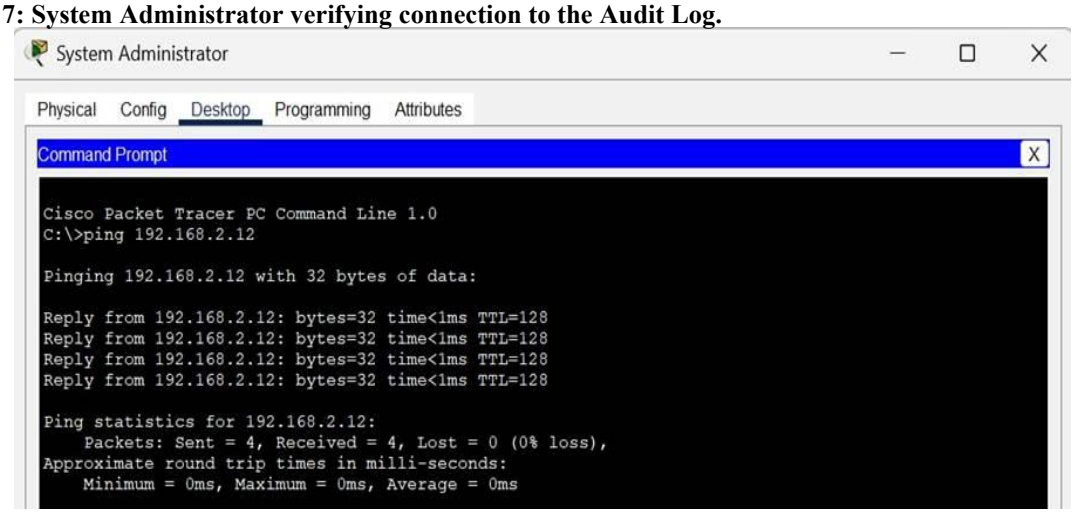
Second, the Government Enforcement node successfully accessed the content source with 0% packet loss (**Figure 6**), proving operational readiness for emergencies.

Figure 6: Authorized Government Enforcement accessing data.



Finally, the System Administrator successfully connected to the Access_Audit_Log server (**Figure 7**), verifying that the audit trail remains accessible for compliance monitoring.

Figure 7: System Administrator verifying connection to the Audit Log.



Conclusion

The simulation empirically proves that the proposed architecture overcomes the limitations of backend-focused systems as it **fails to prevent raw PII capture and exposure at the edge node**. By enforcing access control at the gateway, our system successfully blocks unauthorized access at the source, ensuring "Privacy by Design" without compromising forensic capabilities.

Implementation Challenges & Feasibility

The 3-layer architecture that we proposed provides a unique and very strong solution for the surveillance that prioritizes privacy in Smart Cities. However, changing from being a conceptual design into a practical deployment in a smart city area is indeed a big challenge regarding technical, financial, and ethical aspects. The current section gives a thorough appraisal of our system's feasibility, pinpoints possible obstacles, and presents the findings by recent studies concerning risk management.

Technical Deployment Challenges

One of the main deployment challenges is Hardware Heterogeneity and Retrofitting. Also stated in (Muhammad et al., 2022), the most part of the urban surveillance networks depend on old cameras without an on-board Neural Processing Unit (NPU) or Graphics Processing Unit (GPU) to run the modern deep learning models such as YOLOv8-nano or BlazeFace in real-time.

This brings up a problem, which is that switching out all the working original cameras with the AI smart devices is financially impossible and also is a complicated task. Our planned solution for this, we are proposing a retrofitting deployment model to tackle this issue. Rather than replacing each of the respective sensing units, the city can implement Edge Gateways, like NVIDIA Jetson Nano or Orin Nano units. A single gateway can have up to 4 to 8 old legacy cameras and perform the atomic anonymization task for the cluster. Thus, hardware costs are reduced significantly while "privacy-at-the-edge" remains the main architectural principle.

Another issue would be Blockchain Network Latency and Throughput. While permissioned blockchains like Hyperledger Fabric offer significantly higher throughput than public chains, like Ethereum, they still face latency limitations compared to traditional SQL databases. As highlighted in (Li et al., 2021), that as the number of peers

in a blockchain network increases, the latency can grow, potentially creating a bottleneck during emergency situations where rapid data access is critical.

In high pressure situations, like in mass-casualty or high-speed chase, a delay of even 5 to 10 seconds could be unacceptable. To mitigate this issue, we propose a Hybrid Caching Mechanism. The Access Layer should maintain a secure, short-lived cache of active permissions. Once a user, for example, The Police, is authenticated and authorized via the blockchain for a specific operation, a secure session token is issued that bypasses the blockchain for subsequent requests within a short window. The creation of the session is logged immutably, but individual frame requests during the session are logged asynchronously to prevent latency buildup.

Scalability Concerns

Running deep learning models requires continuous, intensive computation. As mentioned in (Fitwi et al., 2021), it demonstrates that while lightweight models are efficient, their performance degrades as the number of objects in the frame increases. One of the main challenges, in high-density scenarios, such as a crowded protest, the number of "person" and "license plate" bounding boxes the YOLO model must detect, and mask can spike from 5 to 500. This load can cause thermal throttling or frame drops, leading to "privacy leakage" where frames are transmitted unblurred due to lag.

To overcome this obstacle, The Particle Swarm Optimization (PSO) task of offloading capability is critical here. As proposed in our designed architecture, overloaded nodes must inherently detect latency spikes. Using PSO, an edge device can make an intelligent, real-time decision to offload the detection task to under-utilized nearby nodes or a fog layer, ensuring the system scales dynamically with crowd density without compromising privacy.

Another concern brought up is the increase in Storage Growth. Surveillance systems generate petabytes of data. While the Cloud Layer handles video storage, which can be deleted if required, the Blockchain Audit Log is immutable and append-only. Over an extended amount of time, let's say 5 to 10 years, a ledger recording millions of access requests per day will grow to an unmanageable size. To ensure long-term feasibility, our system will implement Ledger Pruning or "Checkpointing." The active blockchain should only maintain the last 12 months of logs for immediate verification. Older logs can be hashed, summarized into a "Merkle Root" snapshot, and archived in cheaper "Cold Storage", like Amazon Glacier.

Cost Analysis

Implementing this system requires a significant upfront investment. Firstly, would be Hardware Cost. High-performance edge computing units (GPUs) are significantly more expensive than standard IP cameras. Next is Integration Cost. The cost of developing custom smart contracts and integrating the "Chaotic Masking" module into firmware is substantial.

The justification for the cost, CapEx is high, as cost of ownership impacts Cost of Non-Compliance. Under the local Data Protection Acts, a single data breach of un-anonymized biometric data can draw millions in fines, and this is without considering reputation damage and loss of public trust. Investing in "privacy-by-design" is the best insurance against these ruinous costs.

Operational Expenditure (OpEx)

The energy consumption of running AI models 24/7, will increase the power consumption of each node. A standard CCTV camera consumes roughly around 5 to 8W, whereas a device running YOLO inference may consume roughly 15 to 25W. Across 10,000 cameras, this energy cost is absurd. To counter this, this increased energy cost is partially offset by Bandwidth Savings. By processing and compressing video at the edge and only transmitting metadata rather than continuous 4K raw streams, the city saves significantly on cellular (4G/5G) data transmission costs, which are often a major component of smart city OpEx.

Ethical Concerns

One of the main ethical concerns is The Risk of Reversibility (Key Management). Our proposal utilizes Reversible Chaotic Masking (video frame encryption as proposed by Giorgi et al), a distinct advantage over destructive blurring because it allows for evidence recovery. However, this creates a "Master Key" vulnerability.

It brings an ethical risk, whereby if the chaotic decryption keys are centralized and the database is breached, the privacy protection is instantly nullified. Our solution for this risk is utilizing an Ethical Guardrail (Shamir's Secret Sharing). Our system will enforce a strict Decentralized Key Management policy. No single official should hold the decryption key. We plan on using Shamir's Secret Sharing, which splits the key into parts. This ensures that "unmasking" creates a high barrier to entry, preventing abuse.

Another known ethical concern is the "Black Box" Problem (AI Bias and Failure). Automated redaction relies entirely on the accuracy of the AI models. As noted in (Fitwi et al., 2021), even lightweight models can suffer from lag or accuracy drops in low-light conditions. Due to this, it could result in 2 scenarios. First scenario, False Negatives. If the model fails to detect a face, Personally Identifiable Information (PII) is leaked. Another scenario being False Positives. If the model incorrectly masks a weapon or a crucial piece of evidence as a "license plate", it could hinder an investigation.

Our strategy to overcome this issue, a random sample of anonymized footage should be reviewed by human auditors to benchmark model performance. Furthermore, the "Confidence Threshold" for masking should be set low, for example, to mask anything with more than 30% probability of being a face, to prioritize privacy, accepting over-masking as a preferable outcome to privacy leakage.

User Adoption and Operational Feasibility

Our new system might take time to adapt due to operational complexity. As shown in (Nuray Baltaci Akhuseyinoglu & Joshi, 2020), more complicated access control models such as RBAC, are typically objected to by the end-users. For example, an officer may consider signing a transaction on the blockchain too inconvenient for a high-pressure situation. Our solution for this, the complication must be abstracted. The User Interface (UI) is designed to be able to plug directly into police dispatch software, activated through standard activities like opening a case file, such that compliance would be unnoticeable by the user.

Another well-known issue would be the struggle to gain the trust of citizens. Citizens are increasingly worried and skeptical of the "smart city" expression, often viewing it as an excuse for surveillance. Our strategy to overcome this hurdle is to provide Public Auditability. What this means is, we allow civil liberty groups or the general public to view a sanitized version of the Blockchain Audit Log, showing that requests were made, without revealing sensitive case details, the city can mathematically prove that the surveillance system is being used lawfully. This transparency is a powerful tool for gaining public trust and distinguishing this solution from authoritarian surveillance models.

5.Evaluation & Discussion

While we believe that our system is already well designed for mass surveillance and maintaining a secure smart city infrastructure compared to alternative approaches, there are still certain inadequacies that may arise. Thus, in this section we provide a thorough analysis of both the strengths and weaknesses of our proposed security framework.

The first possible downside is the operation constraint over frame-by-frame anonymization that might cause unpredictable delays in the overall computational flow. As each frame needs to go through a different technology stack instantly, there is an inherent hold-up between each phase. It can further cause pipeline pauses because no parallelism is achieved. Combined with the atomicity check, the in-computational overhead may lead to extreme energy consumption, reduced throughput, and unnecessary CPU load even when simple frames could be processed faster. Moreover, the all-or-nothing protection might possibly yield unnecessary failures, when there are micro-crashes already happening on the edge devices due to temperature fluctuation, memory limitations, IO delays, and to name a few.

The other bottleneck is the on-edge encryption using the Chaotic Reversible Masking algorithm. By default, the Chaotic Reversible Masking encryption relies on deterministic chaotic maps rather than provably secure alternatives, resulting in vulnerability to brute-force attacks such as known-plaintext and chosen-plaintext attacks. This indicates the hardship in adhering to FIPS, ISO, and NIST criteria for modern encryption. Therefore, CRM in this system is not used as a standalone encryption mechanism but serves as a quick, alternative anonymization at the edge layer. Full cryptographic protection is applied later at the cloud layer using AES-GCM with HSM-managed key.

With all the weaknesses that have been stated, there are also many strengths within the proposed system. The first strength would be performing anonymization at the edge, as the system avoids the necessity of continuously streaming high-bitrate raw footage (e.g., 1080p) to a central server. Instead, the transmitted anonymized stream consumes significantly less bandwidth, effectively mitigating the network congestion risks which are typically associated with large-scale smart city surveillance. This mitigates any Network Congestion risk that is often associated with smart surveillance which allows scalability of surveillance of the system.

Additionally, by performing anonymization at the edge, the system will avoid the necessity of continuous streaming high-bitrate raw footage, for example, at 4k to the central server. Once anonymization and selective frame transformation take place locally, the resulting stream contains only the necessary contextual information and can be encoded at substantially lower bitrates. This reduces bandwidth consumption by an order of magnitude, enabling high-density deployments without saturating uplinks. This mitigates any Network Congestion risks that are often associated with smart surveillance which allows the system to scale to thousands of cameras without crippling the network infrastructure. Collectively, these advantages allow the system to scale horizontally while preserving reliability and performance, ensuring that network infrastructure does not become a bottleneck as the fleet grows.

Besides that, the OpenSSF Model Signing allows identical, referentially transparent cryptographic operations across all edge devices. In contrast to the traditional surveillance system which relies on remote model updates, our solution prevents exposure of multiple backdoors for attack including poison model injection, insecure face recognition model, or degrading detection accuracy subtly. On top of that, the signing can be entirely done on CPU while keeping the signature check less than 5 milliseconds on Raspberry Pi 4. Its offline capability is also a critical component, requiring no cloud server for certification. From a governance standpoint, model signing aligns with zero-trust security principles (NIST, 2020) and modern compliance frameworks such as NIST SP 800-53. Overall, from the research against the industry standards, OpenSSF Model Signing strengthens the security posture of the edge–cloud AI architecture by guaranteeing model integrity, minimizing trust assumptions, and providing a scalable and industry-aligned method for secure model deployment.

Lastly, with the most commercial systems, for example, Verkada and Eagle Eye Networks, operate on a Centralized Model. This architecture exposes a significant privacy risk: during transmission, unprocessed video

frames still contain full PII. This is a huge vulnerability to interceptions, traffic analysis, or metadata leakage. On the other hand, the proposed system adopts a deterministic, lightweight anonymization workflow, where ephemeral memory allocation prevents any data leakage. Because anonymization and encryption occur prior to network handoff, even a successful Man-in-the-Middle (MitM) interception yields only masked, non-identifying frames with no reconstructable biometric content. This not only drastically reduces the attack surface but also ensures privacy-by-design, complying with regulatory expectations such as GDPR's data minimization principle and NIST's PII protection guidelines. Furthermore, eliminating raw PII from the transmission path prevents unauthorized downstream processing, aligns with modern Zero-Trust principles, and positions the system as fundamentally more resilient than traditional cloud-first surveillance models.

6.Conclusion & Future Work

The rapid development of the Internet of Things has been the critical topic of the next generation where everything will be digitalized, while accompanied by numerous security concerns. This study put an emphasis on the mass surveillance aspect of smart cities, entangling Blockchain-Enhanced Audit system, Access Control, and heterogeneous learning models to establish a robust, modular security framework.

The model achieves a scalable architecture by leveraging layer-oriented infrastructure, in contrast to traditional, centralized certificated authorities. It also enhances the data confidentiality and integrity of both the resource-constrained edge devices and cloud storage. Moreover, the model is expected to maintain a consistent process pipeline at the video frame anonymization phase as opposed to conventional models without any dependence on GPU. From the study on existing research and regulatory compliance, this system can be deployed in several IoT environments.

Despite these benefits, several limitations remain. The sequential indivisibility execution at the edge layer might generate intense heat, leading to thermal malfunction. While Reversible Chaotic Masking is efficient on the capacity-limited devices, it is undeniable that the weak encryption remains exploitable. Furthermore, the integration with existing IoT protocols and cloud architecture is yet to be explored, leaving uncertainty in adoption of this system in the future.

Future research should focus on improving parallelism and secure anonymization techniques at the edge layer. Whereas the evolution of the hardware will eventually transcend the capacity limitation of the edge devices, adopting privacy-preserving techniques such as homomorphic encryption and Zero-Knowledge Proof could further enhance confidentiality. Industrial validations across domains like smart infrastructure and supply chain systems will be essential to assess the model's viability and readiness for distribution.

To summarize, this study presents a comprehensive and efficient framework for enhancing the mass surveillance system of smart cities through modularization, intelligence, and decentralization. While its scalability and interoperability are addressed, regulatory compliance and further optimization would be the key to realizing its full impact on employment.

7.References

Akhuseyinoglu, N. B., & Joshi, J. (n.d.). *Access Control Approaches for Smart Cities* . ResearchGate. https://www.researchgate.net/profile/Nuray-Baltaci/publication/341232054_Access_Control_Approaches_for_Smart_Cities/links/5eb4df36299bf1287f75242c/Access-Control-Approaches-for-Smart-Cities.pdf

Badidi, E., Moumane, K., & Ghazi, F. E. (2023). Opportunities, Applications, and Challenges of Edge-AI Enabled Video Analytics in Smart Cities: A Systematic Review. *IEEE Access*, *11*, 80543–80572. https://doi.org/10.1109/ACCESS.2023.3300658

CodeBlue. (2023, February 16). *Audit: MySejahtera Data Breach Affected Three Million Users - CodeBlue*. CodeBlue. https://codeblue.galencentre.org/2023/02/audit-mysejahtera-data-breach-affected-three-million-users/

Fitwi, A., Chen, Y., Zhu, S., Blasch, E., & Chen, G. (2021). Privacy-Preserving Surveillance as an Edge Service Based on Lightweight Video Protection Schemes Using Face De-Identification and Window Masking.*Electronics*,*10*(3),236. https://doi.org/10.3390/electronics10030236

Gao, S., Wu, R., Iu, H. H.-C., Erkan, U., Cao, Y., Li, Q., Toktas, A., & Mou, J. (2025). Chaos-based video encryption techniques: A review. *Computer Science Review*, *58*, 100816. https://doi.org/10.1016/j.cosrev.2025.100816

Giorgi, G., Abbasi, W., & Saracino, A. (2022, March 31). *Privacy-Preserving Analysis for Remote Video Anomaly Detection in Real Life Environments* . Institute for Informatics and Telematics, National Research Council of Italy; Institute for Informatics and Telematics, National Research Council of Italy .https://doi.org/10.22667/JOWUA.2022.03.31.112

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges. *IEEE Access*, *8*(3), 24746–24772. https://doi.org/10.1109/access.2020.2970576

https://www.facebook.com/FutureofPrivacy. (2015). *Student Data and De-Identification - Future of Privacy* Forum. Future of Privacy Forum. https://fpf.org/blog/student-data-and-de-identification/

Huh, J., Kang, J., Woo, J., & Lee, S. (2025). A Novel Intelligent Video Surveillance System Using Low-Traffic Scene-Preserving Video Anonymization. *ACM Transactions on Intelligent Systems and Technology*, *16*(2), 1–24. https://doi.org/10.1145/3709001

Ismail, S. N., Hamid, S., Ahmad, M., Alaboudi, A., & Jhanjhi, N. (2021). Exploring students engagement towards the Learning Management System (LMS) using learning analytics. *Computer Systems Science and Engineering*, *37*(1), 73–87. https://doi.org/10.32604/csse.2021.015261

Jacob, S., Alagirisamy, M., Xi, C., Balasubramanian, V., Srinivasan, R., R, P., Jhanjhi, N. Z., & Islam, S. M. N. (2021). AI and IoT-Enabled Smart Exoskeleton System for Rehabilitation of Paralyzed People in Connected Communities. *IEEE Access*, *9*, 80340–80350. https://doi.org/10.1109/access.2021.3083093

Jhanjhi, N. Z. (2025). Investigating the influence of loss functions on the performance and interpretability of machine learning models. In *Lecture notes in networks and systems* (pp. 480–491). https://doi.org/10.1007/978-3-031-91005-0_43

Kanwal, N., Asghar, M. N., Ansari, M. S., Fleury, M., Lee, B., Herbst, M., & Qiao, Y. (2020). Preserving Chain-of-Evidence in Surveillance Videos for Authentication and Trust-Enabled Sharing. *IEEE Access*, *8*, 153413–153424. https://doi.org/10.1109/access.2020.3016211

Khalil, M. I., Humayun, M., Jhanjhi, N. Z., Talib, M. N., & Tabbakh, T. A. (2021). Multi-class Segmentation of Organ at Risk from Abdominal CT Images: A Deep Learning Approach. In *Lecture notes in networks and systems* (pp. 425–434). https://doi.org/10.1007/978-981-16-3153-5_45

Khandelwal, S. (2017, December 29). *Two Romanians Charged With Hacking Police CCTV Cameras Before Trump Inauguration* . The Hacker News Logo; The Hacker News Logo. https://thehackernews.com/2017/12/police-camera-hacking.html#:~:text=According%20to%20the%20criminal%20complaint,an%20effort%20to%20extort%20money

Kuktelionis, C. (2024). *What is Personally Identifiable Information (PII)?* . Trust Arc; Trust Arc. http://trustarc.com/resource/personally-identifiable-information/

Leong, B. (2023, September 5). *Student Data and De-Identification* . FPF; FPF. https://fpf.org/blog/student-data-and-de-identification/

Li, H., Xiezhang, T., Yang, C., Deng, L., & Yi, P. (2021). Secure Video Surveillance Framework in Smart City. *Sensors*, *21*(13), 4419. https://doi.org/10.3390/s21134419

Loveleen, G., Mohan, B., Shikhar, B. S., Nz, J., Shorfuzzaman, M., & Masud, M. (2022). Explanation-Driven HCI model to examine the Mini-Mental State for Alzheimer's Disease. *ACM Transactions on Multimedia Computing Communications and Applications*, *20*(2), 1–16. https://doi.org/10.1145/3527174

Muhammad, K., Hussain, T., Rodrigues, J. J. P. C., Bellavista, P., de Macedo, A. R. L., & de Albuquerque, V. H. C. (2021). Efficient and Privacy Preserving Video Transmission in 5G-Enabled IoT Surveillance Networks: Current Challenges and Future Directions. *IEEE Network*, *35*(2), 26–33. https://doi.org/10.1109/mnet.011.1900514

Nuray Baltaci Akhuseyinoglu, & Joshi, J. (2020). Access control approaches for smart cities. *Institution of Engineering and Technology EBooks*, 1–40. https://doi.org/10.1049/pbce128e_ch1

Odeh, A., & Taleb, A. A. (2025). Federated Learning and Blockchain Framework for Scalable and Secure IoT Access Control. *Computers, Materials and Continua*, *84*(1), 447–461. https://doi.org/10.32604/cmc.2025.065426

Protecting Personal Data in Smart Cities: The Role of Privacy Tech | TrustArc.(2024).TrustArc. https://trustarc.com/resource/protecting-personal-data-in-smart-cities/

Riskhan, B., Roua, A., Mahaba, B. S., Uswa, D., Gheisari, M., & Sindiramutty, S. R. (2025). Enhancing Diagnostic Accuracy for Breast Cancer Using Classical-Quantum Hybrid and Transfer Learning Technique. *Journal of Soft Computing and Data Mining,* *6*(2), 41–56. https://penerbit.uthm.edu.my/ojs/index.php/jscdm/article/view/22061

Sanjaya, F. N., Balakrishnan, S., Sindiramutty, S. R., & Narputro, P. (2025). XAI Technology in EEG Signal Based Disease Detection Models. *2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC)*, 1–7. https://doi.org/10.1109/icmctc62214.2025.11196271

Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Tee, W. J., Lau, S. P., Jazri, H., Ray, S. K., & Zaheer, M. A. (2024b). IoT and AI-Based Smart Solutions for the Agriculture Industry. In *Advances in computational intelligence and robotics book series* (pp. 317–351). https://doi.org/10.4018/978-1-6684-6361-1.ch012

Sindiramutty, S. R., Prabagaran, K. R. V., Akbar, R., Hussain, M., & Malik, N. A. (2024a). Generative AI for Secure User Interface (UI) design. In *Advances in information security, privacy, and ethics book series* (pp. 333–394). https://doi.org/10.4018/979-8-3693-5415-5.ch010

Sindiramutty, S. R., Tan, C. E., & Wei, G. W. (2024). Eyes in the sky. In *Advances in information security, privacy, and ethics book series* (pp. 405–451). https://doi.org/10.4018/979-8-3693-0774-8.ch017

Weiqi, X., Hooi, S. T. C., Sindiramutty, S. R. a. L., Asirvatham, D. a. L., Kumar, D., & Verma, S. (2024). Surface Anomaly Detection Using Machine Learning Technique. *2024 International Conference on Emerging*

Trends in Networks and Computer Communications (ETNCC), 1–7. https://doi.org/10.1109/etncc63262.2024.10767562

What *is Personally Identifiable Information (PII)? | TrustArc*. (2024). TrustArc. https://trustarc.com/resource/personally-identifiable-information/

Williams, J. (2017, January 30). *D.C. police department hit with ransomware*.CyberScoop. https://cyberscoop.com/washington-dc-ransomware-dc-police-department/

Ying, X., Murugesan, R. K., Sindiramutty, S. R., Wei, G. W., Balakrishnan, S., Kumar, D., & Verma, S. (2024). Scene Text Recognition using Deep Learning Techniques. *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 1–9. https://doi.org/10.1109/etncc63262.2024.10767484

Zhu, H., Chau, S. C.-K., Guarddin, G., & Liang, W. (2022). Integrating IoT-Sensing and Crowdsensing with Privacy: Privacy-Preserving Hybrid Sensing for Smart Cities. *ACM Transactions on Internet of Things*. https://doi.org/10.1145/3549550

Zoonen, L. van. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004